UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/069,714	04/26/2002	Michael John Hill	16673-7	4005

7590 06/21/2005

Clifford W Browning
Woodard Emhardt Naughton Moriarty & McNett
Bank One Center Tower
111 Monument Circle Suite 3700
Indianapolis, IN 46204-5137

EXAMINER	
ALOMARI, FIRAS B	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 06/21/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/069,714	HILL ET AL.	
	Examiner	Art Unit	
	Firas Alomari	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 April 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) *1-10* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _____ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *02/27/2002*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendments

The claim changes for claims 4-7 submitted 02-27-2002 in the preliminary amendment have been accepted.

Specification

1. Applicant is reminded of the proper content of an abstract of the disclosure.

Applicant is reminded of the proper language and format for an abstract of the disclosure.

The abstract should be in narrative form and generally limited to a single paragraph on a separate sheet within the range of 50 to 150 words. It is important that the abstract not exceed 150 words in length since the space provided for the abstract on the computer tape used by the printer is limited. The form and legal phraseology often used in patent claims, such as "means" and "said," should be avoided. The abstract should describe the disclosure sufficiently to assist readers in deciding whether there is a need for consulting the full patent text for details.

The language should be clear and concise and should not repeat information given in the title. It should avoid using phrases which can be implied, such as, "The disclosure concerns," "The disclosure defined by this invention," "The disclosure describes," etc.

The following guidelines illustrate the preferred layout for the specification of an application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC (See 37 CFR 1.52(e)(5) and MPEP 608.05. Computer program listings (37 CFR 1.96(c)), "Sequence Listings" (37 CFR 1.821(c)), and tables having more than 50 pages of text are permitted to be submitted on compact discs.) or REFERENCE TO A "MICROFICHE APPENDIX" (See MPEP § 608.05(a). "Microfiche Appendices" were accepted by the Office until March 1, 2001.)
(f) BACKGROUND OF THE INVENTION.
(1) Field of the Invention.
(2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

2. The disclosure is objected to because on page 3 of the specification, paragraphs 5 refer to claim number. Since the claim numbers and/or subject matter set forth in the claims is subject to change, the claim numbers should be

replaced with the subject matter applicant is referring to. Appropriate Correction is required.

Claim Objections

3. Claim 10 is objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim cannot depend from any other multiple dependent claim. See MPEP § 608.01(n).

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1-10 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding claims 1, 2 and 3: it's not clear to the examiner what is the downstream encryption/decryption module and what is upstream encryption/decryption module and what is the difference between the operation

of the two. Also the claims recite the limitation "begins its operation as soon as part of the result is available" this statement is indefinite.

Regarding claim 5: claim 5 recites the trademark/trade name RSA. Where a trademark or trade name is used in a claim as a limitation to identify or describe a particular material or product, the claim does not comply with the requirements of 35 U.S.C. 112, second paragraph. See Ex parte Simpson, 218 USPQ 1020 (Bd. App. 1982). The claim scope is uncertain since the trademark or trade name cannot be used properly to identify any particular material or product. A trademark or trade name is used to identify a source of goods, and not the goods themselves. Thus, a trademark or trade name does not identify or describe the goods associated with the trademark or trade name. In the present case, the trademark/trade name is used to identify/describe software application method and, accordingly, the identification/description is indefinite.

Regarding Claims 5, 6, 7, 8 and 9: the claims recite the limitation "the so-called private key..... and the so-called public key....." in the claims language. There is insufficient antecedent basis for this limitation in the claim. Even if the limitation specify where and how the key is obtained it's unclear to the examiner how this limitation is used in the invention.

The claim Language must be more specific for Examiner to understand and be able to search for the invention. The claims as presented cause massive

ambiguities, which make examination highly difficult. Examiner will interpret the claims to their broadest reasonable interpretation until a more clear presentation of the claims has been displayed. Examiner will interpret the claims to their broadest reasonable interpretation until a more clear presentation of the claims has been displayed.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-4 are rejected under 35 U.S.C. 102(b) as being anticipated by Coppersmith et al. US (5,768,390).

Regarding claim 1: Coppersmith discloses a method of encryption and decryption using several encryption/decryption modules in series (Col 3, lines 29-33 and FIG.1 and 2), characterized in that the downstream encryption/decryption module begins its operation as soon as part of the result from the upstream encryption/decryption module is available (Col 5, 34-49 and Col 1, lines 41-46).

Regarding claim 2: Coppersmith discloses the method according to Claim 1, characterized in that the downstream decryption module begins its decryption

operation as soon as part of the result from the upstream decryption module is available. (Col 4, line 60 through Col 5, line 8)

Regarding claim 3: Coppersmith discloses the method according to Claim 1, characterized in that the downstream encryption module begins its encryption operation as soon as part of the result from the upstream module is available. (Col 5, lines 34-52 and FIG. 4)

Regarding claim 4: Coppersmith discloses the method according to Claim 1 characterized in that it implements three modules (A1, S, A2),(Col 6, lines 59-64 and item 710 of FIG 7 / three decipherment steps using K1-K3) the central module (S) being of the type with secret symmetric key (k).(Col 6, lines 64-67/ DES is a symmetric key encryption which uses the same keys for encryption/decryption)

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 5-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith et al. US (5,768,390) in view of Menezes, Van Orschot, Vanstone. Hand Book of Applied Cryptography, 1997, CRC Press, 5th Edition, 283-291 hereinafter Menezes.

Regarding claim 5: Coppersmith discloses the method according to Claim 4, characterized in that all the models for encryption/decryption are of the DES type with symmetric keys (Col 3, lines 51-57) but he doesn't disclose the first and the last modules are of RSA types of asymmetric keys with a private key and a public key. However Menezes teaches using of RSA for protecting messages sent over insecure channel where he teaches the using of public key to encrypt the message and private key to decrypt that message (Page 286, 8.4). Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Coppersmith system with the teaching of Menezes to use the RSA algorithm in the encryption modules to substitute for symmetric encryption modules. One would be motivated to do so in order to enable the system to overcome the problem of exchanging the decryption keys securely while maintaining the same level of data confidentiality. Furthermore using symmetric and asymmetric encryption on the same cipher makes it harder for attackers to obtain the private key.

Regarding claims 6 and 9: Menezes teaches using RSA as described in claim 5 where the private key is used for encryption and the public key is used for decryption. (Page 286, 8.1 and 8.3)

Regarding claim 7: Coppersmith discloses the method according to Claim 6, characterized in that the two modules (A1, A2) use the same private key (d, n) and public key (e, n) set. (Col 4, line 60 through Col 5, line 7 / first encryption is performed using K1 and the last encryption is performed using the same K1 as well)

Regarding claim 8: Coppersmith discloses the method according to Claim 6, characterized in that the two modules (A1, A2) use a different set of private (d1, n1; d2, n2) and public (e1, n1; e2, n2) keys.(Col 6, line 59 through Col 7, line 7 / the first module uses K1 and the last module uses K3 rather than K1)

8. Claim 10 is rejected under 35 U.S.C. 103(a) as being unpatentable over Coppersmith et al. US (5,768,390) in view of Goldstein et al. US (6,128,735).

Regarding claim 10: Coppersmith doesn't teach using the method according to Claims 1 to 3, characterized in that it implements three encryption/decryption modules (A1 , A, A2) with asymmetric keys. However Goldstein discloses a method for transferring data having different sensitivity level (see abstract) where he teaches the using of encryption using RSA (Col 3, lines 53-66).

Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was made to modify Coppersmith method with the teaching of Goldstein to implement all the modules in the system to support asymmetric key encryption because using a symmetric key would eliminate the risk of the shared key being compromised during exchange by enabling the system to communicate securely with other systems without by using their public keys. Additionally using asymmetric and symmetric keys in the system enables the system to provide backward compatibility with system that just provide one method for encryption decryption.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Firas Alomari whose telephone number is (571) 272-7963. The examiner can normally be reached on M-F from 7:30 am - 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ SHEIKH can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Firas Alomari
Examiner
Art Unit 2136

FA